METHODOLOGY FOR ANALYSIS OF HYBRID THREATS, TASKS AND DUTIES OF INTELLIGENCE IN THIS PROCESS

YANSISLAV YANAKIEV[1*], ELISLAV G. IVANOV[2]

[1]*Bulgarian Defence Institute "Prof. Tsvetan Lazarov",*
e-mail: y.yanakiev@di.mod.bg

[2]*National Defence College „G. S. Rakovski",*
e-mail: e.ivanov@rndc.com

Abstract. The strategic international security environment remains complex and dynamic. Taking into account the international military-political events, it can be concluded that there is a worsening trend. All this leads to the perception of global and regional destabilization and the appearance of more and more regional conflicts, which subsequently turn into frozen or aggressive conflicts, where the line between peace and war is gradually blurred. Questions related to the nature of hybrid threats and hybrid challenges are becoming increasingly relevant. In parallel, the difficulties of intelligence detection of threats and hazards, as well as the formulation of ways and means of countermeasures against hybrid threats, are increasing. Questions related to the nature of hybrid threats and hybrid challenges are becoming increasingly relevant. In parallel, the difficulties of intelligence detection of threats and hazards, as well as the formulation of ways and means of countermeasures against hybrid threats, are increasing (European Union, 2015). There is a persistent tendency to undertake a variety of open and hidden actions to exert influence, pressure, and control by external forces on the internal political realities of individual countries with the aim of restructuring or making them dependent (Ivanov, 2021).

Keywords: intelligence, intelligence cycle, stages, risks, hybrid threats and hybrid challenges

1. INTRODUCTION

There is a new type of security threat, defined as a hybrid, which manifests itself in the centralized, controlled, and combined use of hidden and non-hidden tactics, as well as of various strategic means and instruments by military and non-military actors, in conventional and/or irregular manner, often keeping anonymous authors. It

* Corresponding author
http://doi.org/10.7546/EngSci.LXII.2025.01.08

includes cyber-attacks, influence capabilities, economic and political pressures, hoarding of energy supplies, and damage to critical infrastructures and public services, but also destabilization strategies (Hagelstam, A, 2018; Torossian, Fagliano, & Görde, 2020; Hoffman, 2007).

The goal of the hybrid strategy carried out by country X is to destabilize an EU Member State (MS) and to stimulate a process of annexation based on separatist activities of a part of the country (region) populated mainly by minority group people (i.e., as it happens in Ukraine now).

Target: Big minority group living in country Y which has close cultural and religious relations with a neighboring country.

Perpetrator: A state actor which supports separatist activities of a minority group in a neighboring country.

Lines/Vectors of the Hybrid attack: Disinformation and propaganda holding statements about planned assimilation policy in country Y that will influence the status of the minority group in terms of prohibition of using the minority language in public spaces, as well as imposing significant constraints on political and religious rights.

- State support for existing or establishment of new political parties and movements as representatives of the minority group.
- State backing of the establishment and the activities of NGOs with official goal work for the protection of the rights of the minority group.
- Sponsoring of a minority group media establishment in country Y and active use of the media in country X to influence the minority group.
- Investments in enterprises, trade organizations, and companies to supply financial support to the representatives of a minority group and their political separatist activities.
- Sponsoring of education of young people from minority groups and religious leaders.
- Imposing economic pressure by cutting the oil and gas supply, as well as economic sanctions concerning the minority rights violation in the country Y.
- Provocation of hatred and tensions between majority and minority groups based on social and economic status and religious differences.
- Coordination with a friendly country Z to impose pressure on country Y to supply the minority group a status of political, economic, and cultural autonomy or to be an independent state.
- Increasing the military presence close to the borders with the country Y, demonstrating the threat of the use of force and determination to support the separatist activities of the minority group in the country Y.
- Affecting the country Y's internal political regime by influencing the election processes.
- Sponsoring local criminal groups or grey area entrepreneurs to decrease the authority of the state security services.

– Organizing and/or sponsoring cyber-attacks against popular, as well as state-important websites and platforms to degrade the authority of the government.

2. MODELLING SCENARIOS OF A HYBRID MULTI-DOMAIN ENVIRONMENT. CHRONOLOGY OF THE SITUATION

2.1 Country X

Country X borders country Y. Country Y has a significant ethnic population that professes religious beliefs and views close to the population of country X. As a pretext for realizing its aggressive intentions, country X, through various means, misinformation, and propaganda criticizes the government of the country Y and its policy towards the minority population. There are allegations about assimilation policy by the country Y's government, the minority religious cults have been destroyed and a ban on the use of the minority language has been passed. In addition, significant restrictions have been imposed on the practice of their religious beliefs in public places and restrictions on their political and cultural rights. The implementation of the hybrid strategy aims at the gradual creation of a regional conflict, secession of the region from the main territory of country Y, and the creation of autonomy.

Another option, depending on the circumstances, is for the conflict to escalate into a frozen one, which could cause tensions in the region at any moment. The strategy of country X also includes a military element of an armed presence near the country Y border, demonstrating strength and readiness for aggressive action to protect the minority group.

Country X is reviewing some of its typical hitherto direct methods of influence considering the international community's heightened sensitivity to possible public scandals and revelations of unregulated interference in the internal affairs of the sovereign state Y.

2.2 Country Y

The grounds of country Y for the existence of preconditions for aggressive actions against it are information and reports from the intelligence agencies, which hold substantiated facts and evidence, based on reliable analytical information provided by the analytical intelligence for organized hybrid aggression by country X.

The reasons and motives for this are short-term manifestations of hybrid threats contained in the hybrid strategy of country X.

They are based on the findings: of conducting disinformation and propaganda campaigns, publishing misleading information in the media and websites in support of minority groups, and profiles on social networks aimed at influencing public attitudes and causing confusion among the population.

The overall assessment of the country's Y intelligence agencies is that the predominant manifestation of these hybrid threats is in the first place in the field of politics, secondly in the field of economics, and lastly in the field of defense.

Overall, the focus is on a minority group in country Y population that has been subjected to an assimilation policy by its government. Due to ethnic cohesion and increasing support through various means, including financial, leads to hesitation and uncertainty among decision-makers.

Another area of more lasting character is the attempts to create a political party, in which representatives of the minority group mainly participate for the purpose of political influence. The group is financially supported by the country X. The use of persons who are citizens of the country Y who are sympathizers of the minority group as „persons of influence" to try to change the political landscape by creating parties and movements with a tendency to take part in the upcoming elections.

A long-term trend is the finding by the intelligence authorities that the economic presence of country X has been strengthened through the establishment of joint trade companies, NGOs, cultural centers, and foundations, not hiding their main idea, namely protecting, and expanding the rights of the minority groups. This economic pressure is also realized in cooperation with another neighboring country, Z, which is the main resource source and supplier for country Y.

Another critical area is the conduct of disinformation and propaganda campaigns and the publication of misleading information in the media of the country Y, Internet sites, minority media, and social networks aimed at influencing public attitudes and awareness of chaos.

All these activities, carried out through regular hybrid threats and hybrid conflicts, are implemented in multidimensional space - land, sea, air, space, and cyberspace, and lead to the implementation of the overall hybrid strategy of country X against country Y.

3. METHODOLOGY FOR INTELLIGENCE ANALYSIS OF HYBRID THREATS

Based on the situation of contradictions and tensions between countries X and Y, it can be assumed what actions should be taken by country Y to protect itself from aggressive covert and overt actions of country X. Through its hybrid strategy X looks to destabilize an EU Member State and to stimulate the process of annexation of a territorial region of the country Y, predominantly populated by a minority population with close ethnic and religious links to the country-of-origin X.

4. PURPOSE AND SUBJECT OF THE GIVEN SITUATION

The subject of the situation is the hybrid threats to the security of country Y to influence a large minority group inhabiting a certain area of its country. The purpose of the situation is to understand the role and place of the intelligence agencies of country Y in detecting the hybrid threats to it, contained in the hybrid strategy of country X.

5. MAIN TASKS OF THE INTELLIGENCE IN RESOLVING THE SITUATION

First task - revealing the nature, content, and identification of the types of military-political threats applied to country Y.

Second task - assessment of the real capabilities of the country Y and the available potential for the implementation of such threats and reveal their nature. Analysis of the issues that decide the duration of their manifestation - short-term or long-term.

Third task - application of the stages of the intelligence cycle in its sequence with a focus on cycles 1 and 2.

Fourth task - distribution of the obtained intelligence task to the responsible operative structures, processing and conducting analytical and information activities.

Fifth task - classification by importance and opportunities for the actual implementation of the hybrid threats coming from country Y.

Sixth task - checking, comparing, and informing the requestor about the results of the obtained and processed intelligence information.

Seventh task - application of a scientific method (SWOT analysis) to compare and verify between scientific validity and practical coherence about the nature of strategic factors and manifestations of hybrid threats. This will help uncover unforeseen circumstances, facts, elements, and statistics related to the hybrid strategy of country X (Heuer, 1999; Ivanov, 2021).

6. METHODOLOGY FOR ANALYZING THE SITUATION

In the first place, these are the results of the processing of information obtained from various sources (closed and open) and especially from the intelligence agencies working in the field. Of particular importance is the activity of the information-analytical bodies of intelligence, which unite in a common analytical intelligence product and represent a united collective work. Of particular importance is the reliability of the final information product, which will help to make informed decisions.

Secondly, through the proposed tools of SWOT analysis, an analytical process can be generated and used for the strategic analysis of modern hybrid risks and threats as an extension that contributes to an effective policy and/or strategy for undertaking

the right countermeasures). This helps to select a proper strategy to counter or neutralize hybrid threats coming from country X to ensure a sustainable balance of country Y's security environment. To compile a SWOT analysis, a list of strategic factors must be generated in relation to the given situation and the applicability of hybrid threats in the security environment. This is possible - the subject is hybrid threats that occur in a particular environment, which is the security environment of country Y. Intelligence analysis can be generated by the approach of country X by constantly watching the elements and factors affecting hybrid threats and their manifestations (How to Do SWOT Analysis, 2021).

7. NATURE OF THE PROBLEM ACCORDING TO THE SITUATION

The dynamic risk stage of development, in which political crises and conflicts are becoming more frequent, the obtained preliminary data and information about the planned aggressive actions by X, are not taken seriously by the leadership of country Y.

As a result of continued activity in this direction, the intelligence found the presence of prerequisites and actually implemented challenges and threats, which are not symmetrical and linear but are mainly asymmetric, nonlinear, network, and hybrid.

Hybrid threats have been identified as the most serious, resilient, and difficult to predict.

The target framework, which is built by the intelligence of country Y, has a general character as the focus is on the following areas where hybrid aggression is expected to be carried out, as the focus on the following features categorized as follows:

- Depending on the nature of the threats - military or non-military.
- Sphere of manifestation - political, military, economic, informational, ecological, ethnic, religious, etc.
- Mode of impact - direct (terrorism, organized crime, corruption, and governance weaknesses) and indirect (climate and energy issues).
- Form of manifestation - real or potential.
- Probability of occurrence - low, medium, and high probability.
- Symmetric or asymmetric - terrorism, illegal trafficking, organized crime, corruption, violence, xenophobia, Islamic fundamentalism.
- Domain of the manifestations - land, sea, air, cyber, or combined.
- By scale - large-scale or limited (regional or local).
- Frequency of manifestations.
- Others.

On this basis, it can be concluded that the intelligence of country Y implements options for detecting hybrid threats based on a combination of forms and means, which may vary depending on the circumstances and content of their manifestations.

Regarding the hybrid feature "Mode of impact" it is the convincing confirmation of increasing in intensity and evolving in nature hybrid threats to country X from country Y. This gives a reason to conclude that the implementation of evolving actions against country X by country Y causes political, economic, energy, social, ethnic, cultural, religious, and other similar in nature and direction problems.

Another essential element in the intelligence reports is the fact that country X has other resources and capabilities for hybrid impact in addition to the existing available ones for developing the hybrid strategy.

Figure 1 shows the stages of the intelligence cycle used by the intelligence agencies in country Y (Sfetcu, 1999).

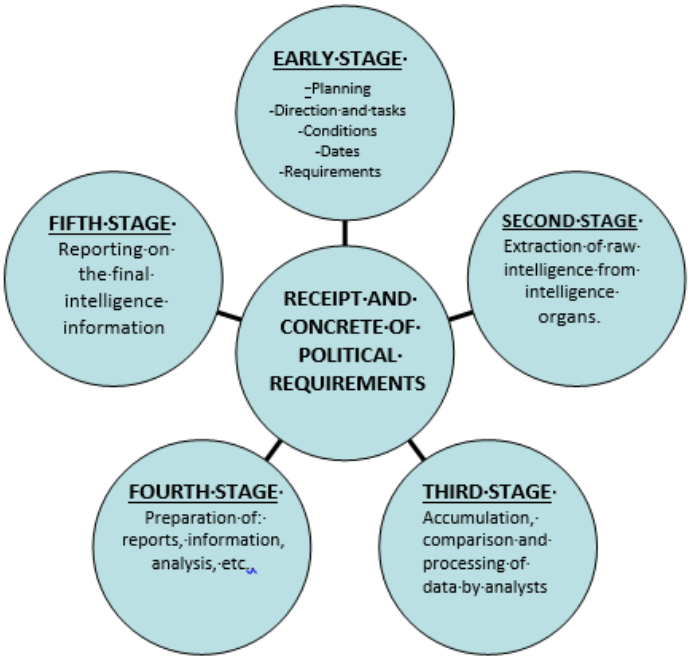

Fig. 1. Phases of the intelligence cycle of country Y

The essence of the functions, tasks, and activities of the intelligence of the country is in the implementation of the defense of the country and the protection of national sovereignty and collective security from external encroachments, risks, and threats (Lazarov, 2009).

To improve efficiency, the conditional intelligence cycle is divided into two main activities:

(1) Acquiring intelligence or activities to gather intelligence information; and;

(2) Analytical intelligence actions.

The process of acquiring intelligence information is implemented through:

(1) Operational intelligence activity;

(2) Electronic intelligence;

(3) Intelligence through images and,

(4) Open-source intelligence.

The analytical intelligence process is carried out by performing information-analytical activities in the implementation of long-lasting information-gathering tasks, which are developed based on received requests from the requestors, analysis of the strategic security environment, long-term trends in its development and allied commitments to the intelligence communities with which it keeps interaction and cooperation, as an EU member state (Moore, 2006).

These two components of the Y countries' intelligence are interdependent and cannot be implemented or function without each other. In the activity so far, increasingly important, and functional weight is given to acquiring intelligence.

This function has been important for the intelligence of country Y, but due to financial and personnel changes, it has recently lost this paramount role.

Greater attention is paid to obtaining information from open sources, which has given analytical intelligence advanced functions.

In the first phase of the intelligence cycle, the planning stage, the intelligence agency of country Y mainly focused its activities on the requirements for the gathering of needed information, and especially on the deadlines for implementation of the task which was to collect data from as many sources as possible sources to compare it upon the receipt.

Once the data was obtained, it had to be checked with the available information in the intelligence agency's database, and a decision had to be made as to its reliability. This is a time-consuming and ungrateful work, but most of the time the information worker processing information is more concerned with comparing and summarizing data than collecting and classifying it.

The main activity of intelligence analysts is to collect, accumulate, process, and analyze the information obtained and, on their basis, to transform it into relevant assessments and conclusions in the form of information documents. This was one of the strengths of country Y's intelligence work.

The comparison of information is an especially important process for another reason. Today, modern technology allows the system to be loaded with an extraordinary amount of information, but the role of the human factor is still extremely important in this process. A significant mistake is the admission of external representatives in this process, which has led to a decline in the quality of analytical products.

Once obtained, compared, and distributed in the information archives, the intelligence information must be processed, with a brief abstract or summary emphasizing the essence.

The interpretation of the information stays the work of the intelligence experts, and the dissemination of the information obtained is the most complex process. It is a

practice for a report, reference, or other information document to consist of correct, prompt, and factual information holding comments and assessments of the specialists.

Of particular importance, however, is the predictive nature that analysts have provided of this information. In principle, the effectiveness of intelligence is based on the fact that it is depoliticized.

One of the mistakes made by the intelligence leadership of country Y is that representatives of the minority group that is the target of the hybrid strategy of country X have been hired in their structures to calm the political tensions in the country. In this way, however, intelligence has become a bureaucratic machine, with the face of obstructing the regulated activities of intelligence, which has been an obstacle with profound consequences. In the context of this situation are the admitted weaknesses, underestimation of the real situation about the security of country Y, and the hybrid intentions of country X have not been revealed in advance. Adequate anticipatory or preventive actions have not been proposed.

The dynamically changing security environment and the fast-moving processes in it, which stand out with a certain ambiguity and difficult predictability, have also had a significant impact on the phases of the intelligence cycle. The rapidly changing hybrid threats posed by country X give reason to specify that the intelligence cycle used by country Y is an open stream that is undergoing change because of the aggressive nature of country X's threats.

For that reason, there is another last stage in the intelligence process of country Y - **The stage of sharing and coordination of intelligence information in the intelligence community**. Thus, the comparison and coordination of important intelligence and prognostic information within the shared responsibility with partner services and structures is of particular importance for country Y to identify effective countermeasures (Turkalanov, 2003).

The analysis shows clearly that hybrid warfare should be countered by the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.

First, hybrid aggressors can be emboldened by the success of carefully calibrated activities that avoid crossing „thresholds„ of decisive response, including through policies of ‘plausible deniability’. While such gains may be dismissed as short-term, they leave indelible marks and create dangerous precedents. The potential of hybrid warfare to create destabilizing effects in the international system requires a strategic response.

Second, hybrid activities should be countered with activities focused on detecting, deterring, and responding taking advantage.

Third, indicator-based warning intelligence is of critical importance to the detection of relevant changes in operational status and it could provide intelligence analysts and decision-makers with an alert – or early warning – of undesirable activity.

8. INTELLIGENCE TOOLS AND TECHNIQUES TO RESPOND TO THE HYBRID THREAT

8.1 Use of artificial intelligence

The ever-increasing computing power for processing arrays of intelligence information, optimizing search engines in areas corresponding to the set tasks for analysis and suitability for a new volume of data and facts from various sources is essential for better adequacy of the hybrid environment, which is applied in a new hybrid security environment.

8.2 Use of UAVs for the purposes of the intelligence

It will respond to the need for constant monitoring and continuous reconnaissance of areas where hybrid manifestations have been found in a rapidly changing operational environment and help operational decision-makers respond in a timely manner with counter-instructions against country X.

8.3 Space systems and means of observation

(Geospatial Intelligence GEOINT), which is the extraction of geographic information and satellite images.

Space monitoring is inherently like that used in aviation monitoring systems. The differences are mainly in the systems and means of monitoring. Space surveillance systems include space and terrestrial parts. The space part consists of satellites for photo, optoelectronic, and radar reconnaissance.

8.4 SIGINT signal intelligence

Refers to the automatic collection of information through the interception and collection of digital data related to intelligence. The collected signals are filtered using discriminators or selectors to determine the criteria that show which data should be stored in the analytical intelligence database.

8.5 Electronic intelligence

Information from Electronic Intelligence, which is often sensitive, is obtained from a complex system of special equipment for the collection and analysis of radio signals and is most often obtained from specialized units. The complexity of this type of information lies in the fact that it is often encrypted and requires the use of cryptanalysis. It is mainly used in cross-checking intelligence and analysis and helps to make informed decisions in crisis and conflict situations to prevent and achieve superiority.

8.6 Machine electronic processing

The use of electronic processing techniques by analysts to improve data collection and aggregation, structure data into categories, and analyze texts in different languages, will contribute to better and timely analysis, risk assessment, and generating forecast models.

Use software models that generate models that predict a future event or development in a hybrid security environment.

As the volume of incoming intelligence increases, so does the accuracy of the predictive nature of electronic processing (Vandepeer, 2014).

9. CONCLUSIONS

1. Having considered the admitted weaknesses in the intelligence of country Y, it is necessary to develop options for the development of the situation and events in the border area between countries X and Y.

2. The identification of the vulnerabilities of critical infrastructure is needed to prevent and protect the national interests of the country Y.

3. To realize this result, the analytical intelligence will rely primarily on the reliability and promptness of intelligence information from the acquiring intelligence agencies, which will allow deciding for the realization of the hybrid conflict.

4. To predict development trends, intelligence management needs to be aware of the vision for the future development of the situation, which requires serious knowledge and skills. The difficulty lies in the fact that it is problematic to overcome old knowledge, which in each situation has led to a certain success based on earlier knowledge.

5. The focus needs to be on the X-Country Hybrid Strategy, which is still in its infancy. This will enable decision-makers not to miss opportunities for an adequate response.

6. Naturally, the most difficult and responsible act of decision-makers is to anticipate hybrid risks and threats leading to a particular hybrid crisis and to supply guidance for the future.

7. The hybrid threats, used by country X are still short-lived and have not transitioned to military-political threats. The prompt analysis and classification of the hybrid threats carried out by country X will allow for the objective and qualitative characterization of the hybrid security environment and take measures to prevent hybrid aggression.

The measures that would be requested to be proposed by the intelligence to the leadership of the country Y to resolve the situation are summarised below.

1. Urgent measures for reorganization of the security system.
2. Reforming law enforcement and law enforcement agencies.
3. Restructuring of the intelligence and counterintelligence services.

4. Changes in the border security services to prevent external influence.
5. Economic and social measures to increase the income of the population.
6. Preventing the development of radicalism and extremism in the country.
7. Urgent consultations on the status of the minority group with full respect for human rights and religious freedoms.
8. Control and prevention of financial dependence, money laundering, and illegal NGOs.

REFERENCES

[1] EUROPEAN UNION, Intelligence Surveillance, ISBN 978-92-9491-045-5, online: fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

[2] A HAGELSTAM, Cooperating to Counter Hybrid Threats (2018) *NATO Review*, **23**, online: https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html [Viewed 2 February 2020].

[3] R. HEUER AND J. JR, Psychology of Intelligence Analysis (1999) Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, ISBN 1 929667-00-0, online: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis.

[4] F. HOFFMAN, Conflict in the 21st Century: The Rise of Hybrid Warfare (2007) Potomac Institute for Policy Studies, Arlington, VA, US.

[5] OCTOPUS, How to Do SWOT Analysis with Competitive Intelligence Questions (2021) online: https://www.octopusintelligence.com/how-to-do-swot-analysis-with-competitive-intelligence-questions/ [Accessed on 24.04.2024].

[6] E. IVANOV, Analytical Intelligence: Methods and Techniques for Information Analytical Expertise (2021) p. 14, National Defense College "G. S. Rakovski", ISBN 978-619-7478-61-7.

[7] V. LAZAROV, Human Intelligence (HUMINT), Sofia (2009) ISBN 978-954-321-576-8 p.13-14.

[8] T. MOORE, Critical Thinking and Intelligence Analysis (2006) p.63, Joint Military Intelligence College, Washington, ISBN 978-1-932946-07-9.

[9] N. SFETCU, Cycle du renseignement, SetThings (2019) online: https://www.setthings.com/fr/cycle-du-renseignement/.

[10] B. TOROSSIAN, L. FAGLIANO AND T. GÖRDE, Hybrid Conflict. Neither War nor Peace (2019-2020) Strategic Monitor, online: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/hybrid-conflict/ [Viewed 21 January 2020].

[11] YURI. TURKALANOV, Intelligence Analysis (2003) p. 20, Sofia.

[12] C. VANDEPEER, Applied Thinking for Intelligence Analysis: A Guide for Practitioners (2014) Air Power Development Centre, Department of Defence, Military intelligence, Commonwealth of Australia ISBN: 978192506204.

Received January 10, 2025